Q80013 - SPECIFICATION TO BE FILED

WHAT IS CLAIMED IS:

1.   A packaged content structure for authenticating a content provider and assuring content integrity, comprising:

an encrypted content portion; and

a header comprising an address from which a certificate of the content provider can be acquired.

2.   The structure as claimed in claim 1, further comprising an electronic signature made through hash coding of predetermined parts of the header and encrypted content portion so as to assure the integrity of the packaged contents.

3.   The structure as claimed in claim 2, wherein only some of the encrypted content portion are hash coded and then included in the electronic signature.

4.   The structure as claimed in claim 1, wherein the header comprises a content provider's name, a content ID, a license provider's URL, and meta-information.

5.   A method of authenticating a content provider and assuring content integrity, comprising :

downloading packaged contents with an electronic signature made thereto into a device of a user through a wired/wireless communication network;

finding a URL address from which a certificate for verification of the signature of the content provider is provided, in a header of the contents;

acquiring the certificate of the content provider after moving to the URL address;

extracting a public key required for verification of the electronic signature from the acquired certificate; and

verifying the electronic signature by using the extracted public key.

6.   The method as claimed in claim 5, wherein the step of verifying the electronic signature comprises applying a hash function to the packaged contents and performing a comparison with the electronic signature.

7.   The method as claimed in claim 5, wherein the electronic signature is made through hash coding of the header and the encrypted content portion and then inserted into the contents.

8.   The method as claimed in claim 7, wherein the electronic signature is made through hash coding of only some of the encrypted content portion and then inserted into the contents.